

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Implementation of the Telecommunications)	
Act of 1996:)	
)	
Telecommunications Carriers' Use of)	CC Docket No. 96-115
Customer Proprietary Network Information)	
and Other Customer Information)	
)	
IP-Enabled Services)	WC Docket No. 04-36

COMMENTS OF EMBARQ

I. INTRODUCTION AND SUMMARY.

Embarq strongly supports efforts to limit the ability of pretexters to obtain unauthorized access to its customers' CPNI. However, additional rules and burdens on telecommunications carriers or consumers are not needed. Indeed, it's been just 3 months since the FCC adopted its *CPNI Pretexting Order*¹ and declared:

In this Order, the Commission responds to the practice of "pretexting" by strengthening our rules to protect the privacy of customer proprietary network information (CPNI) that is collected and held by providers of communications services (hereinafter, communications carriers or carriers)[Citations omitted.]²

The ink is not yet dry on that order. Indeed, the *CPNI Pretexting Order* is not yet fully effective or implemented. Before new burdens are imposed on consumers and carriers, the Commission should allow the *CPNI Pretexting Order* to become effective and then allow time to see if the new rules and the newly adopted Telephone Records and Privacy Protection Act of

¹ *Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) ("*CPNI Pretexting Order*").

² *Id.* at ¶ 1.

2006³ which makes pretexting a criminal offense, have the desired effect. Additionally, at least 5 of the states where Embarq operates as an ILEC have passed criminal pretexting laws, and in other states such legislation is pending.⁴

Embarq and numerous other parties previously noted in this proceeding that the best solution to the problem of pretexting is not to be found in burdening consumers and carriers with additional obligations and steps, but is by going after the root of the problem – the bad actors who are pretexting. Going after the actual known wrongdoer will do considerably more to stem the problem than imposing overly broad burdens on carriers and customers, especially given the paucity of evidence that such action will do little to further the protection of CPNI. The Telephone Records and Privacy Protection Act of 2006 now provides the tools – fines and imprisonment – to do just that.

II. THE FNPRM LARGELY PRESENTS THE SAME QUESTIONS AS RAISED IN THE *EPIC CPNI NOTICE*.

The issues raised and questions asked in the FNPRM issued with the *CPNI Pretexting Order* are much the same as were raised and asked in last year's *EPIC CPNI Notice*: mandatory use of customer set passwords; audit trails; and limitation of data retention. No significant technology advances or areas of vulnerability have occurred in the past year to suggest that the record needs refreshing. Embarq continues to believe it is true, as did other commenters to the

³ Pub. L. No. 109-476, 120 Stat. 3568 (2007) (codified at 18 U.S.C. § 1039)

⁴ See, Florida HB 871 which became effective 7/1/06; Minnesota SF 132 which became effective 8/1/06; Tennessee SB2575 which was signed into law on 5/1/06 and became Public Chapter 566 on 5/12/06; Virginia HB 15181 which was signed on 3/31/06 as Chapter Text 469; and Washington SB 6776 which became effective on 6/7/07 as Chapter 193.

EPIC CPNI Notice, that any additional rules for these three areas are not necessary nor will they effectively shut down the wrongful pretexting activities of data brokers.

The *CPNI Pretexting Order* adopted password requirements for obtaining call detail information via the phone and now seeks further comment on whether passwords should be required for non-call detail CPNI. The answer now, as a year ago, is a resounding no. Mandating passwords for non-call detail CPNI fails to address the problem of pretexting- pretexters focus on obtaining call detail records. Thus, the Commission's actions in the *CPNI Pretexting Order* have already addressed what appears to be the key issue.

Additionally, mandated passwords fall short as a deterrent to pretexting while at the same time burdening customers and carriers. Today, Embarq's customers have an option to use a password, but few do. Since so few customers currently use passwords, establishing passwords for all other customers is a significant undertaking. Most customers already have more passwords than they can remember. Passwords are especially problematic since the majority of Embarq's customers rarely call Embarq, thus increasing the burden of remembering the seldom used password. Password mandates are especially unnecessary for large business customers. Additionally, passwords are not fail proof.

Likewise, the use of audit trails was not a good idea when originally proposed in the *EPIC CPNI Notice* and nothing has changed to indicate that it would be now. There has been no demonstration that audit trails will do anything to stop or prevent data brokers from abusing CPNI. Audit trails will however generate enormous amounts of data which would have to be stored and would require new processes and associated employee training- all at some expense. Given the lack of a demonstrable benefit, no expense or burden on the carriers is justified.

Nor has credible explanation been set forth of how limitations on data retention will deter or prevent pretexting. CPNI consists of many different types of information and is in different forms. This varying type of information has varying retention requirements for tax purposes, GAAP, and other areas of law and regulation. Data retention for telecommunications carriers is not just an FCC issue. Data retention limitations will also expose carriers to potential liability if records cannot be maintained for at least as long as the federal and state statute of limitations periods. The absence of such records will inhibit a carrier's ability to defend itself against baseless claims.

III. PHYSICAL SAFEGUARDS SHOULD NOT BE IMPOSED ON THE TRANSFER OF CPNI.

The Commission seeks comments on whether physical safeguards such as encryption or audit trails should be imposed on the transfer of CPNI between companies, agents, and affiliates. No such safeguards are necessary; there is nothing in the record which demonstrates that such onerous requirements would be an effective tool in preventing pretexting and there is nothing in the record to suggest that breaches of carriers' database security are the cause of or contribute to the pretexting problem.

Additionally, Embarq generally does not transfer CPNI⁵, but rather 3rd party telemarketing agents access Embarq systems where CPNI is stored through secure logons obtained through Embarq's Security group. This 3rd party access does not allow access to the entire customer database at one time, but rather only on a record by record basis when working on a specific customer's account. Contracts with 3rd party telemarketing agents have strict confidentiality clauses which require immediate agent termination and removal from Embarq's

⁵ Except of course at the written direction of the customer.

account for any abuse or misuse of customer information. When an agent is removed from Embarq's account, their logon password and database access is eliminated. Additionally, Embarq has worked with most of the 3rd party telemarketing agents for an extended period of time and is not aware of any breaches of their contractual commitments.

IV. NO COMMISSION RULES ARE REQUIRED FOR THE PROTECTION OF INFORMATION STORED IN MOBILE COMMUNICATIONS DEVICES.

Embarq is an MVNO of wireless communications services and offers its customers a variety of mobile communications devices. Embarq already has adequate protections for customer data that is stored on their devices, and believes most other wireless carriers do too. Customers may erase any and all information from their handsets through three different methods. The manual that is included with each device contains detailed instructions on erasing stored data. Or, customers can use the device itself and be walked through the erasure process. Lastly, customers can call Embarq or visit one of our retail stores to have an Embarq representative walk them through the process. It is true that customers will have to take some steps to protect their own privacy. However, that is no different than what individuals have to do to protect their other private information. Most individuals today have numerous sources of private information other than their telephone records and are learning that vigilance is required to protect it all. Additionally, Embarq performs refurbishing of mobile devices. This process includes the deletion of all stored data including text messages, photographs, call history, etc. The process ensures the destruction of customer information and prevents the unwanted release of same.

V. CONCLUSION.

Embarq believes pretexting is serious business. That it places customers at serious risk is

July 9, 2007

without question. That additional burdens imposed on carriers and, with passwords, on consumers will help further prevent pretexting however is far from clear. What is clear though, is that now is not the time to experiment with such additional burdens.

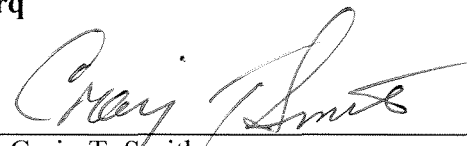
Rather, in the slightly more than a year that has passed since release of the EPIC CPNI Notice, much has happened that should deter pretexting and protect customer information from abuse. The Commission has strengthened its rules on protection of customer privacy with some provisions that are specifically targeted at one of the pretexting problems – telephonic access to CDRs. The rules are not yet fully effective and thus it is too early to know whether they will be successful or whether more regulation is necessary.

Likewise, Congress and several of the States have responded to the pretexting problems by passing new statutes making pretexting a crime and providing punishments of fines and jail time for convictions. It is likely that these legislative activities, more than any regulation, will be the most effective in fighting the bad actors who steal customer's private information. However, it is simply too soon to tell. These new laws and regulations need a chance to be tested before additional unneeded regulations are imposed.

Respectfully submitted,

Embarq

By: _____



Craig T. Smith
5454 W. 110th Street
Overland Park, KS 66211
(913) 345-6691

David Bartlett
Jeffrey S. Lanning
701 Pennsylvania Ave, NW, Suite 820
Washington, DC 20004
(202) 393-7113

July 9, 2007

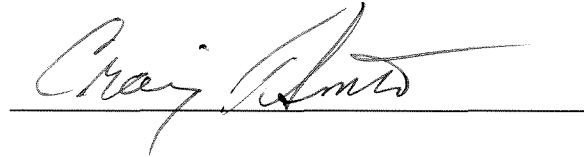
July 9, 2007

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Comments of Embarq was delivered by electronic mail this 9th day of July 2007 to the parties listed below:

Janice Myles
Competition Policy Division
Wireline Competition Bureau
Janice.myles@fcc.gov

Best Copy and Printing, Inc.
445 12th Street, SW.
Washington, DC 20554
fcc@bcpiweb.com.

A handwritten signature in cursive script, appearing to read "Craig R. Smith", is written over a horizontal line.